

REMARKS

The Office Action of June 3, 2005 has been received and its contents carefully noted. The rejection of the independent claims is respectfully traversed for the reasons discussed below.

The Disclosure:

The present application discloses several embodiments of an arrangement which includes a control circuit that either allows or prevents an exchange of signals between a JTAG (Joint Test Action Group) port and a TAP (Test Access Port), in accordance with a security bit stored in a ROM. The control circuit prevents an unauthorized person from circumventing the security bit in the manner described on the first page of the present application.

Independent Claims 1 and 8:

Independent claim 1 recites "a flash ROM that stores a security bit." The Office Action draws attention to a flash memory 5 that is shown in Figure 1 of Iwata et al (hereafter simply "Iwata"), and to the passage at column 4 of the reference, line 64 to column 5, line 6. This passage indicates that a terminal 5a of a gate 5b receives a flash-protect signal FP and a mode signal (indicating either a normal mode or a debug mode). An ordinarily skilled person would understand from the reference that the FP signal is normally input to Iwata's flash memory 5 via the gate 5b to permit or prevent writing into the flash memory 5 (see, for example, the paragraph at column 28, lines 19-26, and claim 11). So the signal FP mentioned in the passage noted in the Office Action is not the "security bit" of claim 1 since it is not stored in Iwata's flash memory 5.

Iwata does store security information, though (possibly in his flash memory 5, although the reference does not appear to expressly state this). A passage that is noted in the Office Action (at column 18, line 47 to column 19, line 10) explains that Iwata's debugging tool 2

requires a user to enter a security code, which is checked against a stored code and, if they do not match, the value of a stored "security level" bit is checked to determine the extent of limitations on further use of Iwata's debugging tool 2. Depending on the value of the security level bit when the wrong security code has been entered, Iwata's debugging tool 2 must either be reset or the flash memory must be erased (column 11, lines 44-58).

It would therefore appear that Iwata's "security level" bit, and not Iwata's FP bit, corresponds to the "security bit" of claim 1. Iwata's security level bit, it bears repeating, controls how the operation of Iwata's debugging tool 2 is to be limited if the security code entered by the operator does not match the stored security code (see column 18, line 59 to column 19, line 6). This control over Iwata's debugging tool 2 serves to protect Iwata's flash memory 5 from unauthorized access (column 19, lines 7-10).

It is instructive to consider what happens, in Iwata's arrangement, if the security code that is entered by the operator does match the stored security code. In that case, the passage from line 47 in column 18 through line 10 in column 19 indicates that data can be read from the memory regardless of the value of Iwata's security level bit. This means that a third-party operator who is able to successfully guess the stored security code, perhaps after a number of trials, or who is successful in a bit of industrial espionage, can access the contents of Iwata's memory. The value of Iwata's security level bit does not matter if the stored security code matches the entered security code. Applicant's approach does not suffer from this drawback. By controlling the signal exchange between a JTAG port and a TAP with a stored security bit, Applicant's approach reliably prevents unauthorized access.

Claim 1 also recites a JTAG port, a TAP, and "a JTAG control circuit controlled by the security bit of the flash ROM, the JTAG control circuit being connected between the JTAG port

and the TAP and allowing or preventing communication of signals between the JTAG port and the TAP depending on the state of the security bit." The Office Action identifies Iwata's element 31 in Figure 5 as a TAP, and Iwata's terminals 11 as a JTAG port. The Office Action also identifies Iwata's element 15 in Figure 5 as "a JTAG control circuit connected between the JTAG port and the TAP ...".

The interpretation of Iwata that is proposed in the Office Action is clearly incorrect. Iwata's Figure 5 shows nothing connected between his terminals 11 and his element 31, which is part of the element 15.

The Mayer reference discloses that a debugger 2 employs an access authorization monitoring device 13 to implement control so as to authorize or deny a read access or a write access to a requested register or memory by an on-chip debug support module, and that the operation of the device 13 itself can be controlled by using a stop signal S. Nothing in Mayer would have led an ordinarily skilled person to modify Iwata so that signal exchange between Iwata's terminals 11 and his element 31 is controlled using a stored security bit.

Independent claim 8 recites "a switch to control on/off between the test port and the central processing unit." On page 4, the Office Action cites two passages in the reference for the proposition that "Iwata teaches controlling on/off between the test port and the central processing unit." It is respectfully submitted, however, that the cited passages do not support this contention, and that Iwata neither discloses nor suggests a switch as recited in claim 8.

Claim 8 also recites "a security control means for selectively turning off the switch if the security bit has been changed to a predetermined state ...". As was noted above, Iwata's security level bit is used to limit the operations of his debugging tool 2 if a stored security code does not match a security code that has been input by an operator. The reference neither discloses nor

suggests turning off a switch that controls whether a signal path between a test port and a CPU is on or off.

The Mayer reference, which was discussed above, does nothing to cure the deficiencies of Iwata. It is therefore respectfully submitted that both references together would not have led an ordinarily skilled person to the invention defined by claim 8.

Independent Claim 4:

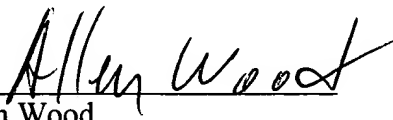
The Office Action rejects independent claim 4 for obviousness on the basis of Iwata, Mayer, and Grimmer, Jr. et al (hereafter simply "Grimmer"). In the Grimmer reference, a bit indicating that a microcontroller 20 is in a security mode is stored.

Independent claim 4 recites "a unit to control on/off between the test port and ... according to the security bit ... ". This is not disclosed or suggested by Grimmer. Nor is it disclosed or suggested by Iwata or Mayer, which have already been discussed. The three references together, therefore, would not have led an ordinarily skilled person to the invention defined by claim 4.

Conclusion:

In view of the foregoing, it is respectfully submitted that claims 1, 4, and 8 are patentable over the cited references. Reconsideration of these claims is therefore respectfully requested.

Respectfully submitted,

A handwritten signature in cursive script that reads "Allen Wood". The signature is written in dark ink and is positioned above a horizontal line.

Allen Wood

Registration No. 28,134

RABIN & BERDO, PC

Customer No. 23995

Telephone: 202-326-0222

Facsimile: 202-408-0924

AW:rw